METHOD FOR STORING DATA IN PAYMENT CARD TRANSACTION

Cross Reference to Related Applications

The present application is a continuation-in-part of U.S. application Serial No. _____ filed September 8, 2000 for Method for Generating Customer One-Time Unique Purchase Order Numbers from a Random Number Generator, which is a continuation-in-part of U.S. application Serial No. 09/640044 filed August 15, 2000 for Method for Generating Customer One-Time Purchase Order Numbers, which is a continuation-in-part of U.S. application Serial No. 09/619859 filed July 20, 2000 for Method for Implementing Anonymous Credit Card Transactions Using a Fictitious Account, which is a continuation-in-part of U.S. application Serial No. 09/571,707 filed May 15, 2000 for Anonymous Electronic Card for Generating Personal Coupons Useful in Commercial and Security Transactions, all of which disclosures are specifically incorporated herein by reference.

The present application is related to the following five patent applications, all of which are specifically incorporated herein by reference, and all of which are being filed concurrently with the present application on the same date: Attorney Docket No. JSF 35.008, entitled "METHOD FOR ALLOWING A USER TO CUSTOMIZE USE OF A PAYMENT CARD THAT GENERATES A DIFFERENT PAYMENT CARD NUMBER FOR MULTIPLE TRANSACTIONS," Attorney Docket No. JSF 35.009, entitled "ELECTRONIC CARD FOR GENERATING A

NEW CARD NUMBER WITH EACH USE WITH LED DISPLAY," Attorney Docket No. JSF 35.010, entitled "METHOD FOR USING ELECTRONIC PAYMENT CARD," Attorney Docket No. JSF 35.012, entitled "METHOD FOR CUSTOMIZING PAYMENT CARD TRANSACTIONS AT THE TIME OF THE TRANSACTIONS," and Attorney Docket No. JSF 35.013, entitled "ANONYMOUS MERCHANDISE DELIVERY SYSTEM."

Field of the Invention

The present invention is in the field of methods for making payments through payment cards.

Background of the Invention

Three forms of money in widespread use today throughout the world are cash, checks and payment cards (debit or credit). Each has distinct advantages, and distinct disadvantages. Cash is readily accepted, easy to use and anonymous, but it does not earn interest, it can be lost or stolen, and it is not always readily accessible. Checks are not always accepted, but they offer many advantages, since they do not have to be written until the time of payment. However, they must be physically presented and they are not anonymous. Payment cards are readily, but not always, accepted, and they offer many advantages over checks. If the card is a credit card, payment can be deferred, but the transaction is not anonymous. If the card is a debit card, payment has usually been made before its use, but it is anonymous. Accordingly, it is

apparent that different types of money have different advantages to different persons in different situations. This may be one reason why all these forms of money are still in widespread use, and are even used by the same persons at different times.

As society and international commerce have become more dependent upon electronic transactions, money has also become more electronic. Many attempts have been made to come up with suitable forms of electronic money that mimic the physical world, or even create new forms of electronic money. However, despite the enormous need for such money, and efforts by some of the best minds and most successful companies in the world, electronic money has suffered many setbacks and been far slower to materialize than many had hoped or predicted. The reasons are many and varied, but some of the obvious reasons are security, ease of use/operation, and unwillingness of the public and/or commerce to make radical changes or embrace new technology and/or procedures. As a result, many efforts, including several potentially promising efforts, have met with failure.

Even though new forms of electronic money have been slow to develop or gain widespread acceptance, electronic payments have still moved forward. Many banks now offer some form of electronic checking. And payment cards have been used for electronic transactions in e-commerce and m-commerce (mobile commerce). Still, there is widespread concern about the safety of such transactions, and recent news stories have uncovered widespread fraudulent activity associated with use of traditional credit card numbers in e-commerce

over the Internet. In addition, there is growing concern about consumer privacy, or lack thereof, due to widespread electronic profiling of consumers who make electronic payments.

Although the media has been quick to cover fraud associated with use of credit cards over the Internet, it is often overlooked, at least by the public and the media (but not the credit card companies), that the majority of fraudulent activity concerning credit cards is not associated with e-commerce activity. Most fraud occurs in the "brick and mortar" world, and the numbers are daunting. Despite many attempts to combat unauthorized or fraudulent use of credit cards, it is estimated that credit card fraud now exceeds hundreds of millions, if not several billion, dollars per year. And this does not even count the cost of inconvenience to consumers, merchants and credit card issuer/providers, or the emotional distress caused to victims of such fraud, or the cost to society in terms of law enforcement and preventative activities.

Accordingly, there is a very real, long-felt need to reduce the amount of fraudulent activity that is associated with credit cards, and this need has only grown more acute as consumers and commerce search for better ways to purchase and sell goods and services via e-commerce and m-commerce. However, any solution needs to be something that is acceptable to the public at large. It should be easy to use. It should not be complicated or expensive to implement. Preferably, it should fit within the existing infrastructure, and not be something that requires a great deal of educational effort, or a radical change in behavior or habits of consumers. In other words, it should be user friendly,

readily understandable and something that does not require a completely new infrastructure, which is a reason suggested by some as to why smart cards have not been widely accepted in the United States.

In addition, it is highly desirable that any solution to such problems be capable of widespread use, in many different platforms, for many different applications.

In U.S. Patent No. 5,956,699 issued in September of 1999, Wong and Anderson were the first to introduce the methodology of a system for secure and anonymous credit card transactions on the Internet. This patent introduced a system which used an algorithm to use one's own selected Personal Identification Number or PIN as one's own de facto digital signature. The algorithm instructs the cardholder how to insert one's PIN into one's valid credit card number before using it for any transactions on the Internet. The resultant scrambled up credit card number, which is tailored by the algorithm to having the same number of digits as before, is rendered useless on the Internet because the PIN insertion algorithm is changed automatically after every transaction. This methodology is not only capable of drastically reducing credit card fraud on the Internet, it is also capable of safeguarding one's anonymity, and thus privacy, in credit card purchases on the Internet.

Since the issuance of U.S. Patent No. 5,956,699, Wong and Anderson have also invented an anonymous electronic card for generating personal Coupons useful in commercial and security transactions, as well as a method for implementing anonymous credit card transactions using a fictitious account

name. The present invention is an extension of these prior inventions that seeks to provide new methods for allowing a user to customize the use of one-time unique numbers that can be used in credit card transactions in the brick and mortar world, e-commerce, m-commerce and in many other applications. Because the methodology is well suited for use in hardware and software applications, it has widespread applicability to many different types of transactions. In addition, the present invention allows a user to include data in the information that is transmitted as part of a normal payment card transaction. This allows the user a great deal of flexibility in customizing use of such a card. In addition, it allows a provider of the card to receive important information as part of the normal processing of a given transaction.

SUMMARY OF THE INVENTION

The present invention is generally directed to a method for transferring a data packet from a user of an electronic card to a money source as part of a payment card transaction. The data packet is stored by an encoder in a magnetic storage medium, which is preferably a second track of a magnetic stripe, read by a standard magnetic stripe reader and submitted to a money source as part of data packet submitted for approval of a given payment card transaction.

In a first, separate aspect of the present invention, a computer in the electronic card executes a computer program, which can be a diagnostic program, to generate information that is stored in the data packet. An example of

such a program is a program that checks on a battery life parameter. The program can generate a warning signal when a low battery condition is detected or a battery life signal related to an estimated remaining battery life of the battery. Such signals can be sent to the money source so that the user can be provided with a replacement electronic card either before or after the battery life drops below a selected threshold.

In other, separate aspects of the present invention, the data packet can be generated by a user of the card. The data packet can contain a customization variable or a user sequence number, or the data packet can be used to obtain the user sequence number.

Accordingly, it is a primary object of the present invention to provide a method for allowing a user to customize a given use of a payment card.

This and further objects and advantages will be apparent to those skilled in the art in connection with the detailed description of the preferred embodiments set forth below.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is related to U.S. Patent Nos. 5913,203, 5,937,394 and 5,956,699, the disclosures of which are all specifically incorporated herein by reference.

The present invention builds upon the disclosure of U.S. application Serial No. 09/571,707 filed May 15, 2000 for Anonymous Electronic Card for Generating Personal Coupons Useful in Commercial and Security Transactions.

This earlier filed application describes an electronic card that contains a magnetic storage medium, which is preferably a magnetic stripe, and an encoder for generating a data packet that is stored in a designated portion of the magnetic storage medium that can be read by a standard magnetic strip reader. It also sets forth a much-simplified theory on magnetic strip technology, especially on how to encode (write) and decode (read) digital data respectively on and off a magnetic stripe used in ordinary credit cards of today. It furthers sets forth data storage mechanics of a magnetic stripe itself, including ANSI/ISO standards for Tracks 1, 2 and 3.

The preferred embodiments of the present invention provide methods to use the encoding technology already disclosed. The methodology is especially well adapted for use in electronic cards used to generate user one-time payment card numbers that are included in a data packet that is sent from a user's electronic card to a money source as part of a payment card transaction.

The present invention stores a data packet in the magnetic storage medium of an electronic card, preferably the magnetic stripe. The data packet is read by a standard magnetic stripe reader and submitted to a money source for approval of the given payment card transaction associated with the data packet. When such a data packet is read and transmitted to a money source, additional information can be conveyed within the data packet, as long as it can be conveniently read by the money source. This is why it is especially preferred that the data packet be encoded in the second track of the magnetic stripe within the field of data that can be read in a normal credit card transaction. Combination of

this capacity for transmission of data with the flexibility provided by use of the encoding technology opens a communication channel for data transmission that can be exploited every time such a transaction takes place.

One way to exploit the communication channel is to use it to directly convey information from the electronic card to the money source. This can be useful in synchronizing the electronic card with the money source. For example, it can be used to provide the money source with a current sequence number of the electronic card. It can also be useful in providing the money source with results of diagnostic test programs that are periodically run by the electronic card's computer, an important example of which is remaining battery capacity Because of the limited capacity of current batteries that are useful in the type of electronic card described herein, it is possible that the battery will cease working before an expiration date of the card if the electronic card is heavily used. To solve this problem, the computer can run a program that measures remaining battery capacity or checks for a battery life parameter and generates a warning signal when a low battery condition is detected. The computer could even run a predictive program estimating when the useful battery capacity will expire based upon past usage, and this program could generate a battery life signal related to an estimated remaining battery life of the battery, which could be sent to the money source. The money source, in turn, can use such diagnostic information to send out a new electronic card to the user before the electronic card runs out of battery life. The same type of communication system can be used for other

diagnostic programs that measure at least one parameter and generate a warning signal when a preselected threshold is exceeded.

Another way to exploit the communication channel is to use it to directly convey information that is generated by a user of the card to the money source. For example, the user could include a customization variable in the data packet. A detailed description of how a customization variable can be used and generated is set forth in Attorney Docket No. 35.012, and a customization variable can also be used in the methods taught in Attorney Docket No. 35.013.

Although the foregoing detailed description is illustrative of preferred embodiments of the present invention, it is to be understood that additional embodiments thereof will be obvious to those skilled in the art. Further modifications are also possible in alternative embodiments without departing from the inventive concept.

Accordingly, it will be readily apparent to those skilled in the art that still further changes and modifications in the actual concepts described herein can readily be made without departing from the spirit and scope of the disclosed inventions as defined by the following claims.